

PUB-NO: FR002679054A1
DOCUMENT-IDENTIFIER: FR 2679054 A1
TITLE: Process and apparatus for exponentiation over GF(2n)
PUBN-DATE: January 15, 1993

INVENTOR-INFORMATION:

NAME COUNTRY
BENJAMIN, ARAZI N/A

ASSIGNEE-INFORMATION:

NAME COUNTRY
FORTRESS U T 2000 LTD IL

APPL-NO: FR09108703
APPL-DATE: July 10, 1991

PRIORITY-DATA: FR09108703A (July 10, 1991)


INT-CL (IPC): G06F015/347

EUR-CL (EPC): G06F007/72 , G06F015/347

ABSTRACT:

The invention relates to a process and an apparatus for exponentiation over GF(2n).

During an exponentiation in a finite field GF(2n), the squaring operation is carried out by constructing a vector. The components of this vector are constituted, alternately, by the components of the vector which is to be squared and by 0. An apparatus provides for the exponentiation in a finite field GF(2n) and includes three registers only, and furthermore has a regular structure which can be produced through very large scale integration.

Application to the authentication of messages, the identification of users and the exchanging of keys. 

(19) RÉPUBLIQUE FRANÇAISE
INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE
PARIS

(11) N° de publication :
(à n'utiliser que pour les
commandes de reproduction)

2 679 054

(21) N° d'enregistrement national :

91 08703

(51) Int Cl³ : G 06 F 15/347

DEMANDE DE BREVET D'INVENTION

A1

(12)

(22) Date de dépôt : 10.07.91.

(30) Priorité :

(43) Date de la mise à disposition du public de la
demande : 15.01.93 Bulletin 93/02.

(56) Liste des documents cités dans le rapport de
recherche : *Le rapport de recherche n'a pas été
établi à la date de publication de la demande.*

(60) Références à d'autres documents nationaux
apparentés :

(71) Demandeur(s) : Société dite : FORTRESS U & T
(2000) LTD. — IL

(72) Inventeur(s) : Arazi Benjamin.

(73) Titulaire(s) :

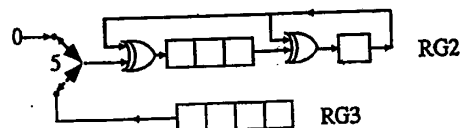
(74) Mandataire : Cabinet Beau de Loménie.

(54) Procédé et appareil d'exponentiation sur $GF(2^n)$.

(57) L'invention concerne un procédé et un appareil d'ex-
ponentiation sur $GF(2^n)$.

Au cours d'une exponentiation dans un corps fini $GF(2^n)$,
l'opération de mise au carré est réalisée par construction
d'un vecteur. Les composantes de ce vecteur sont consti-
tuées, en alternance, par les composantes du vecteur qui
doit être mis au carré et par 0. Un appareil assure l'expo-
nentiation dans un corps fini $GF(2^n)$ et comporte trois regis-
tres seulement, et a en outre une structure régulière qui
peut être réalisée par intégration à très grande échelle.

Application à l'authentification des messages, l'identifi-
cation des utilisateurs et l'échange des clés.



FR 2 679 054 - A1



La présente invention concerne un procédé et un appareil d'exponentiation sur $GF(2^n)$.

$GF(2^n)$ désigne un corps de Galois contenant 2^n éléments, n étant supérieur à 1. Ce corps est un système
 5 numérique qui comporte 2^n éléments et dans lequel les règles d'addition et de multiplication correspondent au modulo arithmétique d'un polynôme irréductible de degré n ayant des coefficients dans $G(2)$, $G(2)$ étant un système numérique dans lequel les seuls éléments sont les nombres
 10 binaires 0 et 1 et les règles d'addition et de multiplication sont les suivantes : $0 + 0 = 1 + 1 = 0$, $0 + 1 = 1 + 0 = 1$, $0 \times 0 = 1 \times 0 = 0 \times 1 = 0$, $1 \times 1 = 1$. L'approche classique pour l'exécution d'opérations dans $GF(2^n)$ comprend la sélection d'un polynôme $P(x)$ de degré n
 15 qui est irréductible sur $GF(2^m)$, avec $m > n$ qui détermine un élément α dans $GF(2^n)$ comme racine de $P(x)$, c'est-à-dire remplissant la condition $P(\alpha) = 0$, et l'affectation de vecteurs unitaires de longueur n ayant des composantes binaires aux éléments $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$.

20 L'exponentiation sur $GF(2^n)$ est une opération qui est nécessaire dans de nombreuses applications décrites dans la littérature, trois d'entre elles qu'on peut se rappeler étant l'authentification des messages, l'identification d'un utilisateur et l'échange de clés.

25 Authentification des messages

Contrairement à un véritable processus de signature numérique, l'authentification des messages nécessite la coopération de l'authentificateur. Dans ce cas, le récept
 30 tionnaire a une assurance en ligne sur l'authenticité d'un message reçu. Ce processus est très utile par exemple dans tous les scénarios dans lesquels un groupe fermé d'utilisateurs veut se protéger contre le monde externe. Un exemple de cas est celui dans lequel un agent transmet un message à une agence, et les deux participants veulent être sûrs
 35 qu'un ordre n'a pas été implanté par un adversaire.

Si l'on appelle X l'expéditeur d'un document M qui doit être authentifié par la partie réceptrice Y et α^a une

clé publique (certifiée) de X, l'authentification est réalisée de la manière suivante (toutes les exponentiations décrites sont modulaires, c'est-à-dire, dans le cas du travail sur GF, qu'elles sont réalisées modulo un polynôme).

- 1) Y génère α^r pour une valeur aléatoire r , et transmet α^r à X. Y calcule aussi $K = (\alpha^a)^r$.
- 2) X calcule $(\alpha^r)^a$ (les deux parties arrivent à une clé $Q = \alpha^{ra}$, qui n'est commune qu'à eux-mêmes).
- 3) X calcule $S = M^k$, et transfère la paire M, S à Y (M peut être chiffré par tout schéma classique ou particulier de chiffrement, donnant le texte chiffré S).
- 4) Y vérifie que M ne peut avoir été transmis que par X par calcul de M^k et par comparaison à S (M et S constituent la paire reçue, K ayant été calculé par Y au pas 1).

Identification d'un utilisateur

Les étapes suivantes constituent une procédure normale dans laquelle une personne X s'identifie vis-à-vis de Y.

- a) X transmet à Y une information non secrète I_{pu} qui est certifiée comme appartenant à X.
- b) Y transmet à X un défi aléatoire C.
- c) X transmet à Y une réponse $R(C, I_{pr})$ dans laquelle I_{pr} est une information privée associée à I_{pu} .
- d) En fonction de I_{pu} , C et R, Y se prouve à lui-même que X est en possession de I_{pr} .

Le scénario précédent est réalisé dans un cas idéal par des opérations sur un corps fini. L'information non secrète I_{pu} est une valeur quelconque α^a dans laquelle l'exposant a constitue l'information privée I_{pr} . Le défi correspond à une valeur quelconque α^r , r étant gardé secret par Y. La réponse R est $(\alpha^r)^a$. Y se prouve alors à lui-même que X est en possession de a , par exponentiation de R à la r^{-1} ème puissance et par comparaison du résultat à α^a .

Echange de clés Diffic-Hellman

Dans le système de distribution de clé publique DH,

les parties X et Y dont les clés publiques certifiées sont α^a et α^b , arrivent toujours à la même clé commune α^{ab} . Les clés de sessions différentes peuvent être créées si une partie X, qui est appelée "l'initiateur" crée une clé
5 différente α^a à chaque session, la signe avec une signature EG, par exemple une signature El-Gamal, et la transmet à l'autre partie Y. La signature de X est nécessaire pour que Y soit sûr qu'il échange réellement une clé de session avec X. Dans ce cas, les clés publiques de X et Y n'ont pas le
10 même rôle. La clé publique de X est nécessaire à Y pour qu'il valide la signature de X sur la valeur reçue α^a . La clé publique de Y est α^b qui, avec α^a , forme la clé secrète de session α^{ab} (les clés publiques de X et Y sont évidemment certifiées par l'autorité de délivrance).

15 Aucune opération de chiffrement n'est impliquée dans ce processus, car l'information échangée α^a n'est pas secrète. Ainsi, lors de la transmission de α^a à Y, X n'utilise pas la clé publique de Y. Cette procédure est tout à fait différente d'un scénario d'échange de clés à
20 base RSA dans lequel une clé secrète de session créée par l'initiateur est signée par lui-même et chiffrée par la clé publique du destinataire.

Dans d'autres cas aussi, on peut utiliser une opération d'exponentiation sur un corps fini ou un corps de
25 Galois. La possibilité du travail sur $GF(2^n)$ a été souvent remarquée dans la technique, par exemple dans l'article de C.C. Wang et al. "VLSI Architectures for Computing Multiplication and Inverses in $GF(2^m)$ ", [IEEE Trans. on Comput., Vol. C-34, pages 709-716, 1985], dans l'article de T. Beth
30 et al. "Architectures for Exponentiation in $GF(2^n)$ " [Advances in Cryptology-Eurocrypt'86, LNCS 263, pages 302-310], et dans l'article de P.A Scott et al. "Architectures for Exponentiation in $GF(2^m)$ " [IEEE J. Sel. Areas Commun., vol. SAC-6, pages 578-586, 1988]. Un procédé et un
35 appareil de calcul et une manière de réaliser des additions, la mise au carré et la multiplication dans une

arithmétique sur un corps de Galois sont décrits dans le brevet des Etats-Unis d'Amérique n° 4 587 627.

Des circuits d'exponentiation sur $GF(2^n)$ ont été décrits dans la technique, par exemple dans le document précité de P.A. Scott et al. Un exemple d'un tel circuit convenant à l'exponentiation sur $GF(2^4)$ par raison de simplicité, est schématiquement représenté sur la figure 1. Ce circuit travaille sur la base du polynôme standard. Il comprend quatre registres. Le vecteur B qui doit être mis au carré est conservé dans RG3. Le facteur A par lequel le vecteur doit être multiplié est conservé dans RG1. A constitue aussi l'élément du corps qui doit être soumis à l'exponentiation. RG2 fait partie d'un circuit de multiplication à registre à décalage à rétroaction linéaire LFSR. RG4 désigne un registre tampon dans lequel A est mémorisé lorsque B est mis au carré, l'opération étant réalisée par duplication de B dans le registre RG1 et traitement comme facteur par lequel B lui-même est multiplié. En d'autres termes, la mise au carré est traitée comme une multiplication d'un vecteur par lui-même. Toute variante de ce type de circuit doit toujours contenir quatre registres lors du travail sur la base de la norme, dans la technique antérieure, à cause de la manière utilisée pour l'exécution de l'opération de mise au carré. On a aussi décrit dans la technique des cas dans lesquels trois registres seulement sont utilisés, dans l'article de T. Beth et al. "Architectures for Exponentiation in $GF(2^n)$ " [Advances in Cryptology-Eurocrypt'86, LNCS 263, pages 302-310] et dans le brevet cité des Etats-Unis d'Amérique n° 4 587 627, mais dans le cas d'une exponentiation non sur la base de la norme mais sur la base normale, et dans ce cas la mise au carré est réalisée par un simple décalage cyclique. Cependant, dans ce cas, comme dans le circuit schématiquement représenté sur la figure 2, en plus de trois registres, d'autres circuits sous forme d'au moins n-1 portes OU-exclusif sont nécessaires. Ces circuits sont représentés sur la figure 2 dans un rectangle en traits interrompus. Ces

circuits équivalent à au moins un registre supplémentaire, si l'on utilise des registres dynamiques comme décrit dans la suite.

L'invention a pour objet l'exécution d'une exponentiation sur $GF(2^n)$ avec une quantité réduite de circuits, à la fois au niveau macroscopique, puisqu'un registre entier est éliminé, et au niveau microscopique, puisque les registres sont réalisés sous forme de registres dynamiques. La structure modulaire facilite en outre la réalisation des circuits.

L'invention a aussi une application plus particulière dans la réalisation de l'exponentiation sur $GF(2^n)$ pour l'utilisation de trois registres seulement et sans introduction de circuits excessifs.

L'invention a donc pour objet la réalisation de l'exponentiation avec une réduction des circuits et avec une structure cellulaire plus régulière.

L'invention a aussi pour objet de permettre la mise en oeuvre de systèmes à clés publiques sur $GF(2^n)$ qui nécessitent une taille bien plus grande de paramètres, pour une complexité cryptographique comparable, sans nécessiter une augmentation des ressources matérielles.

L'invention repose sur la considération du fait que la mise au carré est une opération linéaire sur $GF(2^n)$. Dans le procédé d'exponentiation selon l'invention, l'opération de mise au carré est réalisée par construction d'un vecteur dont les composantes sont en alternance les composantes du vecteur à mettre au carré et 0.

Plus précisément, le procédé selon l'invention met en oeuvre la mise au carré d'un facteur ayant n composantes par construction d'un vecteur ayant $2n-1$ composantes qui sont en alternance celles du vecteur à mettre au carré et 0. Plus précisément, un vecteur $\chi = (c_0, c_1, c_2, \dots, c_{n-1})$ est mis au carré par construction du vecteur $\chi^2 = (c_0, 0, c_1, 0, c_2, 0, \dots, 0, c_{n-1})$. Le vecteur χ^2 n'existe jamais avec sa longueur totale puisqu'il est réduit modulo un polynôme primitif par les insertions alternatives de 0.

De préférence, la construction du vecteur au carré selon l'invention est réalisée par transmission des composantes du vecteur à mettre au carré, appelé dans le présent mémoire "vecteur de base", à un registre et par insertion
5 d'un 0 entre chaque couple d'éléments successifs du vecteur de base pendant son décalage dans le registre. Comme une multiplication doit aussi être réalisée dans un circuit d'exponentiation, le registre auquel les composantes sont transmises est avantageusement une partie d'un circuit de
10 multiplication.

De manière correspondante, un appareil d'exponentiation sur $GF(2^n)$ selon l'invention comporte un dispositif destiné à mettre un vecteur de base au carré (le vecteur étant tel que défini précédemment), ce dispositif comprenant
15 un dispositif destiné à mémoriser le vecteur de base, un dispositif destiné à recevoir les composantes du vecteur au carré, et un dispositif destiné à transmettre en alternance, au dispositif de réception, les composantes du vecteur de base et le nombre 0. De préférence, le dispositif de transmission en alternance comporte un dispositif
20 de commutation qui connecte en alternance le dispositif de réception au dispositif de mémorisation de vecteur de base et à une source de 0. De préférence, le dispositif de mémorisation du vecteur de base est un registre et le
25 dispositif destiné à recevoir le vecteur au carré fait partie du circuit de multiplication LFSR.

L'appareil selon l'invention comporte un dispositif destiné à exécuter l'opération de multiplication afin qu'il complète l'algorithme de mise au carré et de multiplication.
30 L'opération est réalisée de préférence par utilisation d'un circuit supplémentaire qui n'est pas essentiellement différent par sa structure et son fonctionnement du dispositif correspondant des circuits d'exponentiation de la technique antérieure et qui comporte un dispositif, en
35 général à registres, destiné à mémoriser le vecteur -appelé dans la suite "vecteur facteur"- par lequel le vecteur de base doit être multiplié. Pendant l'opération de mise au

carré, le circuit supplémentaire est éventuellement déconnecté par mise à 0 de portes ET qui sont incorporées. Comme l'indique la suite, un circuit d'exponentiation de ce type, destiné à assurer l'exponentiation sur $GF(2^n)$, comporte
5 deux cellules ou unités de structure qui ne sont pas identiques. Comme les corps finis dans lesquels on opère ont un degré n qui est bien plus élevé et peut être de l'ordre de plusieurs milliers, les cellules ou unités de structure doivent être répétées de nombreuses fois. Dans un
10 mode de réalisation de l'invention, ceci est évité et d'autres avantages sont obtenus simultanément.

Dans une telle forme de l'invention, la phase de division de l'opération de multiplication modulaire est réalisée d'une nouvelle manière qui permet l'utilisation de
15 circuits beaucoup plus simples que ceux qui sont nécessaires dans les procédés décrits dans la technique antérieure, par exemple dans le brevet des Etats-Unis d'Amérique n° 4 587 627. Plus précisément, le polynôme qui constitue le modulo de la multiplication modulaire, au lieu
20 d'être fixe et prédéterminé, peut être défini et changé à volonté. La multiplication modulaire est ainsi réalisée par un simple décalage.

Un circuit de ce mode de réalisation de l'invention comprend donc un dispositif de mémorisation des composantes
25 du polynôme primitif modulo qui est le diviseur dans la phase de division de la multiplication modulaire, et un dispositif de commande de la multiplication modulaire par l'intermédiaire des composantes.

De préférence, un circuit de ce mode de réalisation
30 de l'invention comprend un circuit de multiplication LFSR et le dispositif de commande de la multiplication modulaire comporte un dispositif de commande des rétroactions vers le circuit de multiplication LFSR.

De manière plus avantageuse, le dispositif de
35 mémorisation des composantes du polynôme primitif est constitué d'éléments d'un registre qui sont connectés chacun à une porte équivalente ET, les portes ET réglant

les rétroactions vers les portes équivalentes OU-exclusif du circuit de multiplication LFSR.

Un circuit d'exponentiation selon l'invention peut comporter de nouveaux dispositifs de mise au carré, définis
5 précédemment, et dans ce cas, la phase de division de l'opération de mise au carré modulaire est réalisée de la même manière que la phase de division de la multiplication modulaire par utilisation du même dispositif pour la mémorisation du polynôme primitif et du même dispositif de
10 commande de rétroaction.

Dans ce mode de réalisation de l'invention, le circuit comporte de préférence un seul type de cellule ou unité répétitive de structure, la cellule comprenant une porte OU-exclusif, un premier élément de registre placé en
15 série avec la porte OU-exclusif, un second élément de registre, et une porte ET destinée à recevoir une rétroaction et à la transmettre à la porte OU-exclusif, et un troisième élément de registre connecté à la porte ET pour la commande de la rétroaction.

20 Cependant, dans une variante, différents dispositifs de mise au carré peuvent être utilisés, par exemple ceux qui sont représentés sur les figures 1 et 2.

Les éléments de registres indiqués précédemment peuvent être des bascules statiques, mais ils peuvent être
25 différents de celles-ci. Comme tous les registres sont constamment déplacés et mis à zéro et en conséquence effacés naturellement, des registres de type dynamique peuvent être utilisés comme éléments de mémoire, sans organe de commande de mémoire, et ceci constitue une autre
30 caractéristique de l'invention. Une structure d'un registre dynamique à décalage est décrite dans la suite.

En outre, dans les registres dans lesquels une porte OU-exclusif ou NON-OU-exclusif est placée entre les cellules de décalage, ces éléments logiques peuvent être
35 utilisés comme éléments d'amplification dans les registres.

D'autres caractéristiques et avantages de l'invention seront mieux compris à la lecture de la description

qui va suivre d'exemples de réalisation, faite en référence aux dessins annexés sur lesquels :

les figures 1 et 2 représentent schématiquement deux circuits d'exponentiation sur $GF(2^4)$ selon la technique
5 antérieure ;

la figure 3 représente schématiquement un circuit de mise au carré $GF(2^4)$ selon l'invention ;

la figure 4 représente schématiquement un circuit d'exponentiation selon un mode de réalisation préféré de
10 l'invention ;

la figure 5 représente schématiquement un circuit d'exponentiation dans un autre mode de réalisation préféré de l'invention ;

la figure 6 représente un circuit d'exponentiation
15 selon un autre mode de réalisation préféré de l'invention ;
et

les figures 7 et 8 représentent schématiquement deux structures d'éléments de registre selon d'autres modes de réalisation de l'invention.

20 Les figures 1 et 2 ont été déjà rapidement décrites et elles parlent d'elles-mêmes pour l'homme du métier. On se réfère maintenant à la figure 3 qui représente schématiquement un circuit de mise au carré sur $GF(2^4)$, les opérations étant générées par $f(x) = 1 + x^3 + x^4$. Le
25 vecteur de base est conservé dans un registre RG3. La référence 5 désigne un commutateur qui alterne entre une position basse dans laquelle il déplace les composantes du vecteur de base de RG3 vers le registre RG2 alors que, en position haute, il transmet le nombre 0 à RG2. Un vecteur
30 au carré est ainsi créé dans RG2, ses composantes étant en alternance les composantes du vecteur de base et 0. Ce circuit de mise au carré n'a pas la phase de multiplication pour l'exponentiation et il n'est donc pas utilisé en général tel quel ; néanmoins il constitue un aspect indé-
35 pendant de l'invention et il est revendiqué en lui-même dans le présent mémoire.

Un circuit d'exponentiation dans un mode de réalisation préféré de l'invention est représenté schématiquement sur la figure 4. Sur celle-ci, RG3 désigne un registre dans lequel le vecteur de base $\beta = (b_0, b_1, b_2, \dots, b_{n-1})$ est mémorisé. Le vecteur facteur $\alpha = (a_0, a_1, a_2, \dots, a_{n-1})$ est mémorisé dans le registre RG1. Les références 10 et 11 désignent deux commutateurs. Pendant la phase de multiplication qui est réalisée dans ce cas de manière classique, le commutateur 10 est dans la position basse et fait partie du circuit de multiplication alors que le commutateur 11 est en position haute. Pendant la phase de mise au carré, le commutateur 10 est en position haute et sépare le circuit du registre RG1 par transmission de 0 aux portes ET 12. Le commutateur 11 alterne entre ses deux positions. Lorsqu'il est en position basse, une composante du vecteur de base est transmise de RG3 à RG2. Lorsqu'il est en position haute, RG3 est déconnecté de RG2 et un 0 est transmis dans ce dernier. Le vecteur $\beta^2 = (b_0, 0, b_1, 0, b_2, 0, \dots, 0, b_{n-1})$ est ainsi construit à partir du contenu de RG2 après $2n-1$ décalages. On note que RG3 est décalé à la moitié de la vitesse de RG2 ou en d'autres termes le temps de mise au carré est doublé, par rapport aux circuits connus décrits, et est porté à $2n$ cycles d'horloge à la place de n cycles. Cette augmentation de la durée de l'opération est cependant insignifiante en partie compte tenu de l'économie de circuits qui est obtenue par élimination de l'un des registres de la technique antérieure.

Le circuit représenté sur la figure 4 peut être réalisé avec des registres à décalage dynamiques fabriqués à l'aide d'une fraction des transistors utilisés dans une réalisation statique semblable. Etant donné la dimension propre limitée d'une pastille montée sur une carte à mémoire, l'utilisation possible de ces registres peut être une considération essentielle. Le défaut de ces registres est qu'ils se vident en un temps court (d'environ 1 ms) à

moins qu'ils ne subissent un décalage fréquent qui renouvelle leur contenu.

Pendant la multiplication, le contenu de RG1 est fixe alors que le contenu de RG3 est décalé dans RG2. Dans le cas de registres qui ont une longueur d'environ 1 000 bits et une fréquence d'horloge dépassant 1 MHz, le cycle total prend moins d'une milliseconde et, pendant cette période, le contenu du registre RG1 n'est pas perdu. Comme la multiplication est toujours suivie d'une mise au carré, pendant laquelle RG1 est déconnecté (l'interrupteur 10 est en position haute), il peut circuler pendant que RG2 et RG3 exécutent la phase de mise au carré. Des mises au carré successives peuvent se produire et pendant ce temps RG1 circule toujours.

Les registres RG2 et RG3 peuvent évidemment être de type dynamique car ils subissent constamment un décalage.

On a noté que l'invention permettait l'utilisation de trois registres seulement à la place de quatre dans le cas des circuits de la technique antérieure de la figure 1 et des circuits analogues.

Le circuit de la technique antérieure de la figure 2 comporte aussi trois registres seulement, mais il nécessite des portes OU-exclusif supplémentaires qui augmentent les circuits matériels d'une manière correspondant à au moins un registre dynamique supplémentaire. Ce qui est pire est la très grande irrégularité introduite par le câblage de ces portes OU-exclusif, limitant la possibilité de la réalisation de circuits VLSI efficaces (circuits intégrés à très grande échelle).

Des circuits selon le mode de réalisation de l'invention décrit précédemment comportent deux cellules ou unités de circuit encadrées en traits interrompus et indiquées sur la figure 4 par les références 13 et 14 respectivement, différant par leurs structures de portes OU-exclusif (ces portes ayant deux entrées dans la cellule 13 et trois dans la cellule 14), ce fait affectant la régularité du circuit. Si l'exponentiation doit être

réalisée sur $GF(2^n)$ avec $n < 4$, les portes doivent être répétées un grand nombre de fois en pratique. Ceci rend assez peu commode la réalisation VLSI. Cet inconvénient est supprimé dans un autre mode de réalisation préféré de l'invention schématiquement représenté sur la figure 5, dans lequel la phase de mise au carré ne diffère pas de celle qu'on vient de décrire, mais la phase de division de la multiplication modulaire est réalisée d'une nouvelle manière différente. La structure de ce mode de réalisation permet aussi l'exécution de la phase de multiplication de l'algorithme d'exponentiation par un seul décalage.

Le circuit de la figure 5 comporte encore trois registres RG1, RG2 et RG3. La référence 21 indique encore un commutateur correspondant au commutateur 11 de la figure 4 et travaillant de manière analogue dans l'opération de mise au carré. RG1 conserve des polynômes primitifs qui, avec les portes ET 22, commande la structure de rétroaction du registre LFSR RG2. Le commutateur 20 transmet le contenu du registre LFSR dans la ligne de rétroaction pendant la multiplication-mise au carré, et dans le registre RG3 lorsque le contenu du registre LFSR doit être mis à nouveau au carré. Cependant, dans ce cas, pour que l'exponentiation soit mise en oeuvre sur $GF(2^n)$ avec $n < 4$, une seule cellule ou unité de structure entourée en traits interrompus sur le dessin et désignée par la référence 23 doit être répétée un nombre aussi grand de fois que nécessaire, si bien que la structure du circuit est simplifiée et la réalisation VLSI est facilitée.

Les caractéristiques et avantages de la forme d'invention représentée par le mode de réalisation de la figure 5 peuvent être montrées clairement par considération de son utilisation pour le chiffrement. Dans les systèmes habituels de chiffrement, on peut déterminer un terminal qui est en communication avec un certain nombre d'abonnés à un système. Chaque abonné a sa propre carte à mémoire. Des messages sont transmis du terminal vers les cartes et

inversement, et des clés publiques et privées sont utilisées.

Le théorème suivant a été établi par l'inventeur.

Théorème : si f_1 désigne un polynôme primitif de degré n et
 5 α_1 est sa racine sur $GF(2^n)$, si f_2 est le polynôme minimal
 de $(\alpha_1)^Y$, f_2 étant aussi une primitive, si α_2 est la racine
 de $f_2/GF(2^n)$, et si P est une matrice $n \times n$ dont la i ème
 ligne est $(\alpha_1)^{iY}$ avec $i = 0, 1, \dots, n-1$, on a alors
 $(\alpha_2)^Z P = (\alpha_1)^{YZ}$ pour toute valeur de z .
 10 (Note : $(\alpha_1)^Y$ et $(\alpha_2)^Z$ indiquent que l'exponentiation est
 réalisée modulo f_1 et f_2 respectivement, et en outre f_2 est
 une primitive si $\text{pgcd}(2^n-1, Y) = 1$).

On suppose que $(\alpha_1)^X$ et $(\alpha_1)^Y$ sont des signaux créés
 au niveau d'une carte à mémoire et d'un terminal respecti-
 15 vement, α_1 étant la racine sur $GF(2^n)$ d'un polynôme pri-
 mitif f_1 , accepté en commun par tous les participants.
 Diverses applications de chiffrement ont été suggérées dans
 lesquelles $[(\alpha_1)^Y]^X$ a été calculé au niveau de la carte
 $[(\alpha_1)^X]^Y$ a été calculé au niveau du terminal. Pour
 20 $\text{pgcd}(2^n-1, Y) = 1$, f_2 est le polynôme primitif minimal de
 $(\alpha_1)^Y$. Compte tenu du théorème

$$(1) (\alpha_2)^X = [(\alpha_1)^X]^Y P^{-1}$$

pour la matrice P définie dans le théorème.

Il faut noter que le calcul du côté gauche de
 25 l'équation (1) désigne des exponentiations modulo f_2 de sa
 racine α_2 . Ainsi, lors du calcul de $(\alpha_2)^X$ par exécution de
 l'algorithme de mise au carré et de multiplication, la
 "multiplication" par α_2 est obtenue par un seul décalage.

Les lignes de la matrice P^{-1} du côté droit de
 30 l'équation (1) sont $(\alpha_2)^{iZ}$, avec $i = 0, \dots, n-1$, et
 $z = Y^{-1} \text{mod}(2^n-1)$.

Maintenant, d'après ce qui précède, le terminal, au
 lieu de soumettre $(\alpha_1)^Y$ à une carte, peut soumettre le
 polynôme minimal f_2 de $(\alpha_1)^Y$ et la carte calcule alors
 35 $(\alpha_2)^X$. La carte soumet alors au terminal sa valeur α_1^X et
 le terminal calcule $[(\alpha_1)^X]^Y P^{-1}$, et arrive ainsi au même
 résultat.

Une paire clé secrète-clé publique $\{y ; f_2\}$ est créée par sélection initiale d'une valeur y telle que $\text{pgcd}(2^n - 1, y) = 1$, puis par création du polynôme minimal f_2 de α^y . La quantité de calcul nécessaire pour le calcul de f_2 pour une valeur donnée α_y ne dépasse pas une seule opération d'exponentiation.

Par rapport à l'opération complète habituelle d'exponentiation modulaire réalisée aux deux extrémités, l'approche suggérée permet des multiplications (et non la mise au carré) pour un décalage au niveau de la carte, ceci étant compensé par $n-2$ multiplications supplémentaires et jusqu'à $n-1$ additions au niveau du terminal. En plus de l'économie de temps, il existe aussi une certaine réduction des circuits matériels au niveau de la carte et l'obtention d'une structure cellulaire plus régulière qui facilite la réalisation VLSI.

La clé publique f_2 transmise par le terminal est le polynôme primitif qui commande les connexions de rétro-action de RG2. La valeur reçue f_2 est conservée dans le registre RG1. La carte doit assurer l'exponentiation de la racine α_2 de f_2 à la x ième puissance (l'opération est réalisée modulo f_2). L'utilisation de l'algorithme de mise au carré et de multiplication assure la multiplication du contenu de RG2 par α_2 par décalage du registre une seule fois.

Par observation du circuit de la figure 4, on note que la phase de multiplication est réalisée par $2n$ décalages, car le contenu de RG2, destiné à être multiplié par l'élément du corps d'exponentiation, doit d'abord être décalé dans RG3 puis décalé à nouveau dans RG2, si bien qu'il faut au total $2n$ décalages. Ces $2n$ décalages sont remplacés dans ce cas par un seul décalage de RG2 car la multiplication est réalisée dans RG2 sans décalage initial de son contenu à l'extérieur.

Le registre RG3 conserve l'élément qui doit être porté au carré pendant l'exponentiation. (La mise au carré est réalisée par commutation en alternance 10 de la manière

déjà décrite). Cet élément a été formé avant que le contenu de RG2 ne le soit et a été décalé dans RG3. Les registres RG2 et RG3 peuvent être naturellement réalisés sous forme de registres dynamiques à décalage car ils assurent un
5 décalage constant. RG1 peut aussi être un registre dynamique à décalage dont le contenu est renouvelé par circulation alors que le contenu de RG2 est transmis (par l'intermédiaire de S2) à RG3.

Lors de la multiplication comme dans le mode de
10 réalisation de la figure 5, la réalisation de la mise au carré peut mettre en oeuvre tout procédé de mise au carré sur la base de la norme, puisque le procédé suggéré pour la multiplication par un seul décalage est indépendant de la réalisation de la mise au carré. On peut utiliser le
15 circuit de la figure 1. Le nombre de registres dans ce cas est encore égal à quatre puisque le registre RG1, qui conserve le terme produit, est remplacé par un registre qui commande les connexions de rétroaction de RG2.

Pour la régularité de la structure, les trois
20 registres à décalage sont construits par des répétitions de la cellule représentée sur la figure 5. Cette cellule est identique en principe à la plus petite des deux cellules encadrées sur la figure 4. Mis à part l'économie possible de temps offert par le circuit de la figure 4, il existe
25 aussi une certaine réduction des circuits et l'obtention d'une structure cellulaire plus régulière qui facilite la réalisation VLSI.

Il est intéressant de comparer le fonctionnement du circuit de la figure 5 à celui de la figure 2. Le premier
30 travaille sur la base de la norme (polynôme) et le second sur la base normale. Le premier exécute une opération de multiplication en un décalage alors que le second exécute une opération de mise au carré en un décalage. Le second circuit est plus rapide car

35 a) pendant l'exponentiation, le nombre d'opérations de mise au carré est en moyenne deux fois celui des multiplications,

b) le second circuit exécute une multiplication en n décalages alors que le premier réalise la mise au carré en $2n$ décalages.

La figure 6 représente un circuit d'exponentiation dans lequel la multiplication est réalisée comme dans le mode de réalisation de la figure 5, mais la mise au carré est réalisée selon la technique antérieure. Le circuit travaille par mise en oeuvre du principe du circuit d'exponentiation de la figure 1, avec l'option éventuelle de la figure 5, permettant une bonne flexibilité pour la sélection de la structure de rétroaction, c'est-à-dire l'utilisation de polynômes primitifs à modulo différent. L'avantage d'un tel circuit peut être l'exécution de la phase de multiplication dans l'algorithme d'exponentiation par mise au carré et multiplication, en un seul décalage. La mise au carré est encore réalisée par multiplication de deux copies de l'élément qui doit être mis au carré. Ces deux copies sont conservées dans les registres RG1 et RG2. Il faut noter que le registre RG4, utilisé sur la figure 1 pour la mémorisation de l'élément qui doit subir l'exponentiation pendant la phase de mise au carré, n'est pas nécessaire dans le circuit de la figure 6.

La figure 7 représente un circuit d'une cellule d'inversion qui peut être utilisée dans un registre à décalage dynamique très long de numéro pair. Deux cellules sont représentées sur la figure. Les condensateurs 31 et 32 qui sont indiqués ne sont pas obligatoirement des éléments séparés mais peuvent être constitués par des capacités naturelles du circuit. Un inverseur de structure classique est désigné par la référence 30. Des tensions C_{vdd} et C_{vss} peuvent leur être appliquées. Un transistor 35 de passage est monté en série avec eux. L'inverseur 30 est placé en alternance à un état de fonctionnement et de non-fonctionnement, par réalisation en alternance de l'excitation et de la déconnexion de C_{vdd} et C_{vss} . Pendant la phase de non-fonctionnement, le transistor est mis à l'état conducteur.

La figure 8 représente un élément à décalage qui peut être utilisé dans des registres dans lesquels un signal OU-exclusif ou NON-OU-exclusif pilote chaque cellule de registre. La porte OU-exclusif ou NON-OU-exclusif 40 est mise à l'état de fonctionnement ou de non-fonctionnement par excitation et déconnexion en alternance de C_{vdd} et C_{vss} avec transmission du même type d'amplification que celui qui est assuré par l'inverseur du mode de réalisation de la figure 7. Dans ce cas encore, un transistor 41 de passage est monté en série avec la porte, la capacité convenable étant indiquée symboliquement à nouveau par des références 31 et 32.

Bien qu'on ait décrit un certain nombre de modes de réalisation de l'invention à titre illustratif, il faut noter que l'invention peut être mise en pratique d'un certain nombre d'autres manières sans sortir de l'esprit ni du cadre des revendications annexées.

REVENDICATIONS

1. Procédé d'exponentiation dans un corps fini $GS(2^n)$, caractérisé en ce que l'opération de mise au carré est réalisée par construction d'un vecteur dont les composantes sont en alternance les composantes du vecteur à mettre au carré et 0.

2. Procédé selon la revendication 1, caractérisé en ce qu'il comprend la mise au carré d'un vecteur ayant n composantes par construction d'un vecteur ayant des composantes qui sont en alternance les composantes du vecteur à mettre au carré et 0.

3. Procédé selon l'une des revendications 1 et 2, caractérisé en ce qu'il comprend la transmission des composantes du vecteur de base à un registre et l'introduction d'un 0 entre chaque couple d'éléments successifs du vecteur de base pendant le décalage dans le registre.

4. Procédé selon l'une quelconque des revendications 1 à 3, caractérisé en ce qu'il comporte en outre la multiplication du vecteur de base par un vecteur facteur.

5. Procédé de multiplication modulaire, caractérisé en ce que le polynôme qui constitue le modulo de la multiplication modulaire est défini et modifié à volonté.

6. Procédé selon la revendication 5, caractérisé en ce que la multiplication est réalisée en un seul décalage.

7. Appareil d'exponentiation dans un corps fini $GF(2^n)$, caractérisé en ce qu'il comprend un dispositif destiné à assurer la mise au carré d'un vecteur de base, ce dispositif comprenant un dispositif de mémorisation du vecteur de base, un dispositif de réception des composantes du vecteur de base, et un dispositif destiné à transmettre en alternance, au dispositif récepteur, les composantes du vecteur de base et 0.

8. Appareil selon la revendication 7, caractérisé en ce que le dispositif de transmission en alternance comprend un commutateur qui connecte alternativement le dispositif de réception au dispositif de mémorisation du vecteur de base et à une source de 0.

9. Appareil selon l'une des revendications 7 et 8, caractérisé en ce que le dispositif de mémorisation du vecteur de base est un registre et le dispositif de réception du vecteur de base est une partie d'un circuit de multiplication LFSR.

10. Appareil selon l'une quelconque des revendications 7 à 9, caractérisé en ce qu'il comprend un circuit destiné à exécuter l'opération de multiplication et qui comporte un dispositif essentiellement en forme de registre, destiné à mémoriser le vecteur facteur, et un dispositif destiné à déconnecter le dispositif de mémorisation du vecteur facteur pendant la phase de mise au carré.

11. Appareil selon la revendication 10, caractérisé en ce que le circuit destiné à exécuter l'opération de multiplication comprend des portes ET et un dispositif destiné à transmettre 0 aux portes ET.

12. Appareil de multiplication modulaire, caractérisé en ce qu'il comporte un dispositif de mémorisation des composantes du polynôme primitif modulo, qui est le diviseur dans la phase de division de la multiplication modulaire, et un dispositif destiné à commander la multiplication modulaire par les composantes.

13. Appareil selon la revendication 12, caractérisé en ce qu'il comprend un circuit de multiplication LSFR, et en ce que le dispositif de commande de la multiplication modulaire comporte un dispositif de commande des rétroactions vers le circuit de multiplication LFSR.

14. Appareil selon la revendication 12, caractérisé en ce que le dispositif de mémorisation des composantes du polynôme primitif sont des éléments d'un registre qui sont connectés chacun à une porte ET, les portes ET commandant les rétroactions aux portes OU-exclusif du circuit de multiplication LSFR.

15. Appareil d'exponentiation, caractérisé en ce qu'il comprend un dispositif de mise au carré selon la revendication 5 et un appareil de multiplication selon la revendication 12.

16. Appareil selon la revendication 15, caractérisé en ce que le dispositif de mémorisation du polynôme primitif et le dispositif de commande de rétroaction sont communs aux dispositifs destinés à exécuter la mise au carré et à réaliser la multiplication.

17. Appareil selon l'une des revendications 15 et 16, caractérisé en ce qu'il ne comporte qu'un seul type de cellule ou unité répétitive de structure, la cellule comprenant une porte OU-exclusif, un premier élément de registre monté en série avec la porte OU-exclusif, un second élément de registre, une porte ET destinée à recevoir une rétroaction et à la transmettre à la porte OU-exclusif, et un troisième élément de registre connecté à la porte ET pour la commande de la rétroaction.

18. Appareil selon l'une quelconque des revendications 7 à 17, caractérisé en ce que les éléments de registre sont de type dynamique.

19. Appareil selon la revendication 18, caractérisé en ce qu'une porte OU-exclusif ou NON-OU-exclusif est placée entre des cellules successives de décalage des registres, et des éléments logiques sont utilisés comme éléments amplificateurs dans ces registres.

20. Registre dynamique à décalage, caractérisé en ce qu'il comporte une répétition de cellules, la cellule amplificatrice comprenant un inverseur, un transistor de passage et un dispositif destiné à mettre en alternance l'inverseur dans des phases de fonctionnement et de non-fonctionnement.

21. Registre selon la revendication 20, caractérisé en ce qu'une porte OU-exclusif ou NON-OU-exclusif est utilisée comme inverseur.

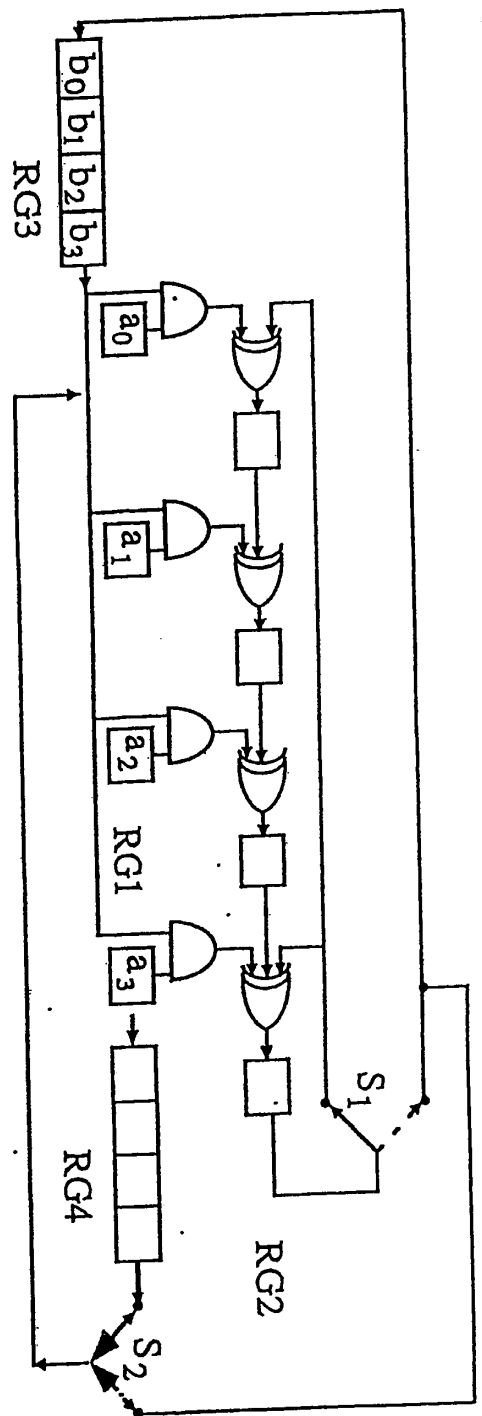


Fig. 1

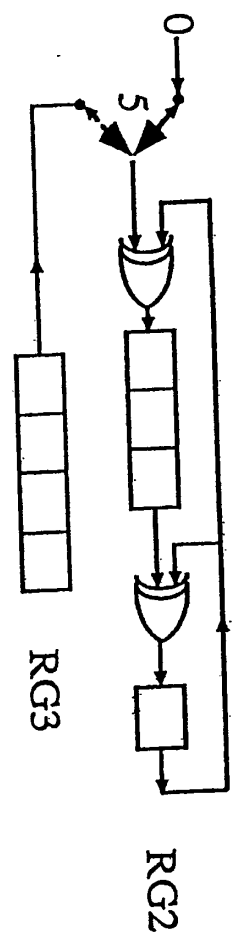


Fig. 3.

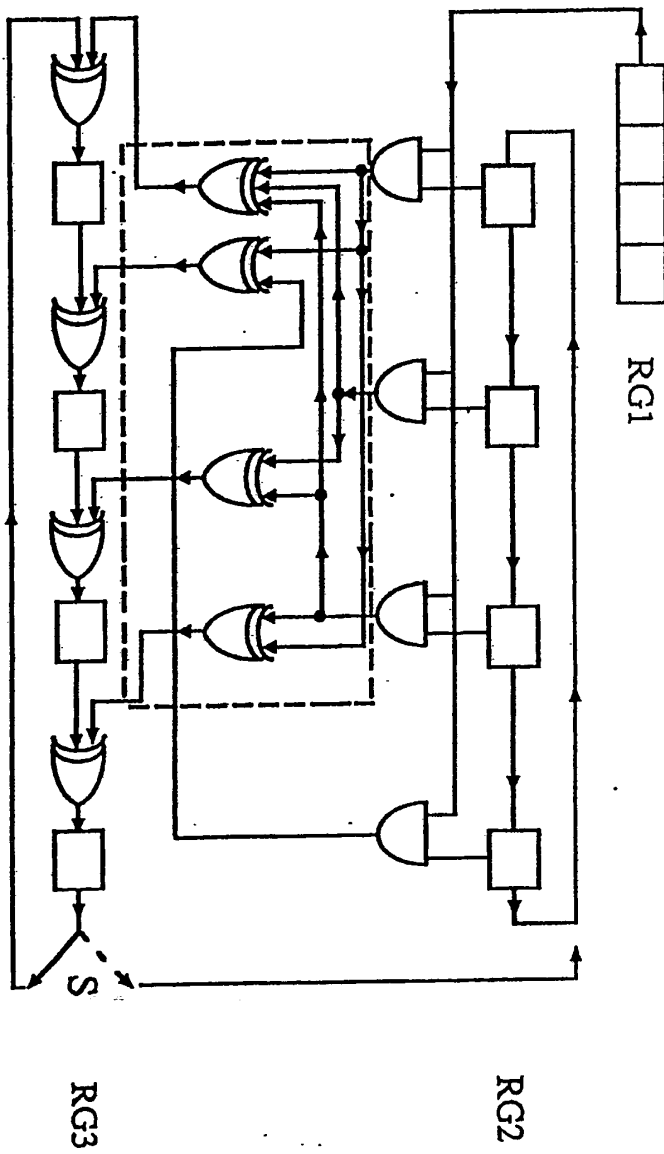


Fig. 2.

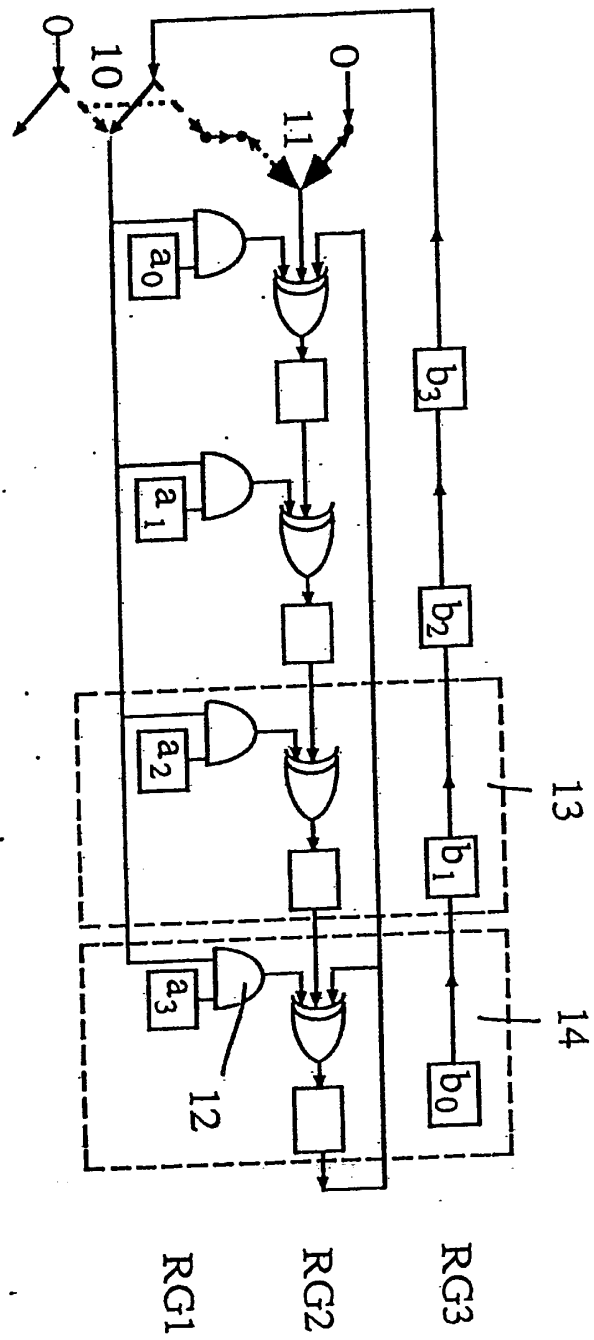


Fig. 4

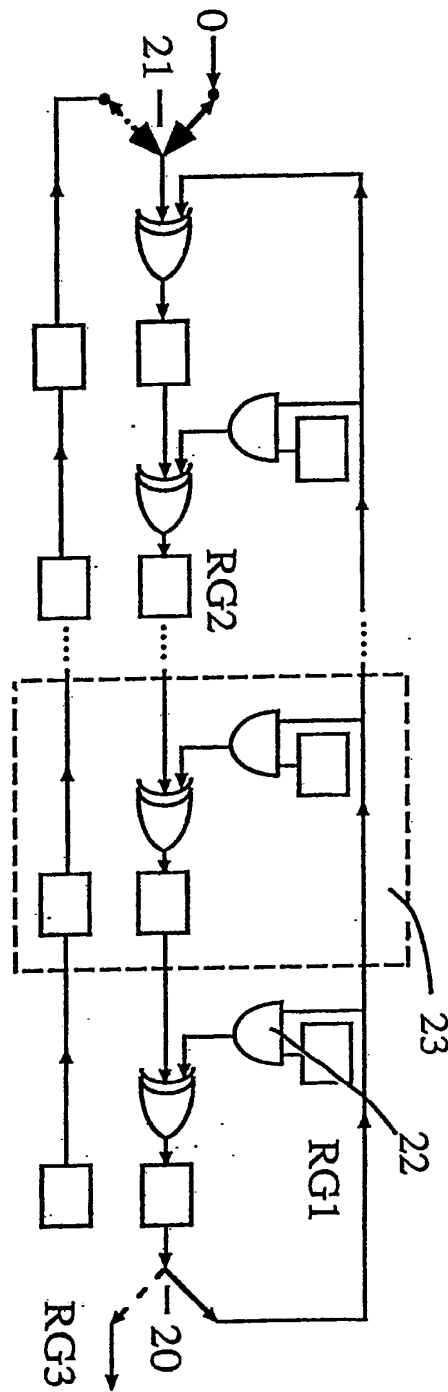


Fig. 5.

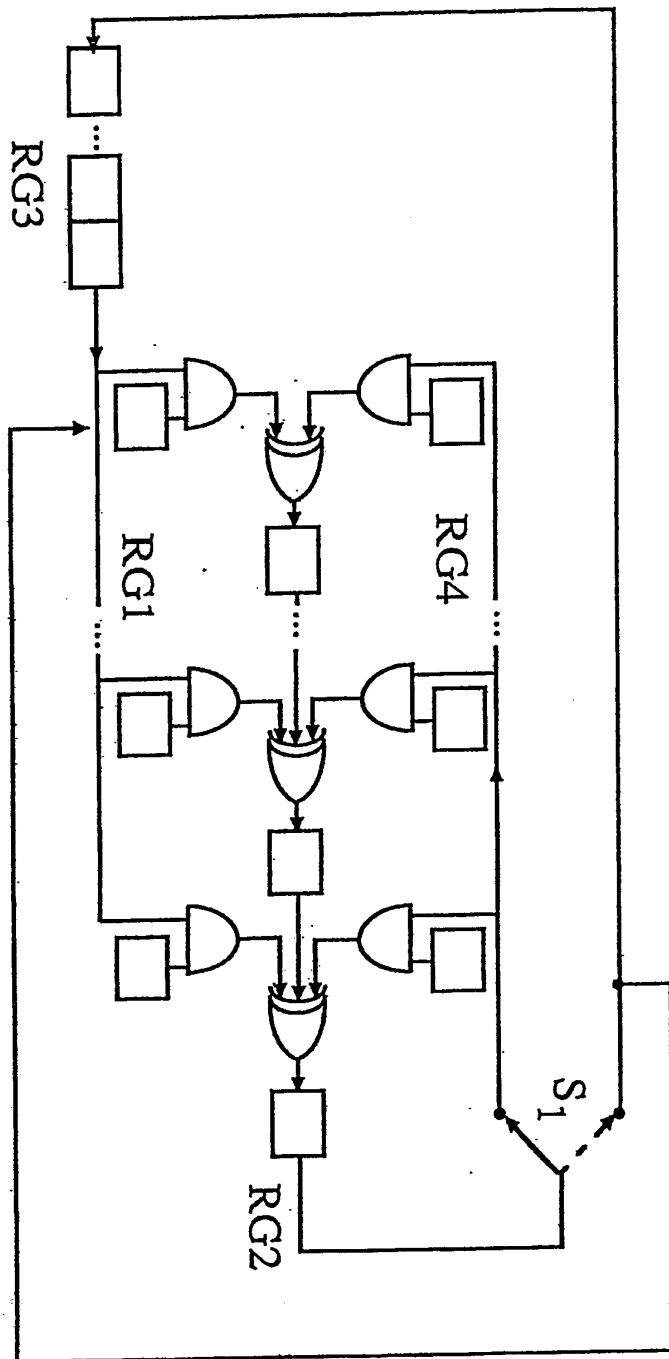


Fig. 6

